

Wie Replicated Cloudflare Access zur Remote-Entwicklung nutzt



Dieser Artikel basiert auf einem Gastbeitrag von Marc Campbell und Grant Miller, den Mitbegründern von Replicated. Eingehende Informationen dazu, wie Campbell und Miller Cloudflare Access und Argo Tunnel zur Entwicklung einer Cloud-basierten IaaS-Lösung genutzt haben, finden Sie im Cloudflare Blog.

Es besteht kein Zweifel, dass die Welt immer mehr über das Internet verbunden ist und dass Bereitstellungsumgebungen immer komplexer werden. Es liegt auf der Hand, dass es nur eine Frage der Zeit ist, bis die gesamte Softwareentwicklung über das Internet und in Einklang mit ihm erfolgt.

Replicated wurde im Jahr 2014 gegründet und ist ein Unternehmen für Infrastruktursoftware, das sich darauf konzentriert, ein neues Modell für die Bereitstellung von Unternehmenssoftware zu ermöglichen, die sogenannte Kubernetes Off-The-Shelf (KOTS) Software. Das Ziel von Replicated ist es, den Benutzern die Installation und den Betrieb von Software von Drittanbietern zu erleichtern, damit das Senden von Daten an Mehrmandanten-SaaS-Provider nicht die einzige Möglichkeit ist, die Dienste dieser Anbieter zu nutzen.

„Wir glauben, dass es auf einfache Weise möglich ist, die Anwendungen sicher und ohne großen operativen Aufwand zu Ihren Daten zu bringen", so Campbell und Miller.

Die Herausforderung

Bei Replicated muss die Entwicklungsumgebung auf Kubernetes laufen, da KOTS in Kubernetes ausgeführt wird und den Lebenszyklus von Anwendungen von Drittanbietern im Kubernetes-Cluster verwaltet. Für die Erstellung und Validierung des Produkts benötigt ein Entwickler Zugriff auf einen Cluster.

Als das Entwicklungsteam von Replicated mit dedizierten Front-End-Entwicklern und anderen Spezialisten erweitert wurde, die nicht durch den Aufbau und die Wartung ihres eigenen Clusters abgelenkt werden sollten, entpuppte sich die Komplexität der Verwaltung einer lokalen Umgebung

Wichtigste Ergebnisse

- Entwickler können Entwicklungstools von überall auf der Welt ohne VPN erreichen
- Die Entwicklungsumgebung von Replicated läuft jetzt vollständig auf IaaS
- Die Mitarbeiter haben dieselbe nahtlose Login-Erfahrung, egal auf welche Arbeitsplatzanwendung sie zugreifen

als immer größere Belastung. Replicated musste vereinfachen, um die Produktivität der Entwickler aufrechtzuerhalten.

„Wir verloren jede Woche mehrere Stunden, weil Entwickler Probleme in ihrer lokalen Umgebung beheben mussten", erklären Campbell und Miller. „Wenn ein Front-End-Entwickler (von dem nicht erwartet wurde, ein Kubernetes-Experte zu sein) Probleme hatte, musste er sich an einen Back-End-Entwickler wenden, um Hilfe zu erhalten. Das beanspruchte nicht nur die wertvolle Zeit von einer, sondern von zwei Personen. Wir brauchten etwas Besseres."

Auf der Suche nach einer Lösung, die einfach zu implementieren und zu warten wäre, wandte sich Replicated an Cloudflare. Ursprünglich hatte das Unternehmen Cloudflare für DNS und DDoS-Schutz genutzt, mit der Zeit aber begonnen, weitere Cloudflare-Dienste einzusetzen, um seine eigenen Dienste verfügbar und sicher zu halten.

"Cloudflare Access bietet eine Authentifizierungsmethode im BeyondCorp-Stil, die sicherstellt, dass die Umgebung von überall auf der Welt ohne die Verwendung eines VPN erreicht werden kann."

MARC CAMPBELL AND GRANT MILLER
Mitbegründer

Replicated nutzt Cloudflare, um seine Entwicklungsumgebung in der Cloud zu sichern

Um seine Entwicklungsumgebung auf IaaS-Ressourcen (Infrastructure-as-a-Service) umzustellen, hat Replicated eine Lösung entwickelt, die Cloud-basierte Infrastrukturkomponenten verwendet, für deren Zugriff und Sicherheit Cloudflare Access und Argo Tunnel eingesetzt werden. Das bedeutet, dass sich die gesamte Entwicklungsumgebung des Unternehmens in der Cloud befindet.

Dadurch hat Replicated die Zeit reduziert, die ein Entwickler für die Fehlerbehebung in seiner lokalen Umgebung aufwenden muss. Jeder Entwickler im Team kann nun auf eine vollständige Entwicklungsumgebung zurückgreifen – auch wenn er nicht über fundierte Kubernetes-Kenntnisse verfügt.

„Diese Konfiguration hat mehrere Vorteile gegenüber einer herkömmlichen Bereitstellung", so Campbell und Miller. „Zum einen hat der Server keine öffentliche IP-Adresse und es müssen keine Ports im Google Load Balancer geöffnet sein, auch nicht für SSH. Die einzige Möglichkeit, sich mit diesen Servern zu verbinden, ist über den Argo Tunnel, der mit Cloudflare Access gesichert ist. Access bietet eine Authentifizierungsmethode im BeyondCorp-Stil, die sicherstellt, dass die Umgebung von überall auf der Welt ohne die Verwendung eines VPN erreicht werden kann."

Cloudflare Access lässt Sicherheitsbedenken verschwinden

Replicated kann nun eine Richtlinie schreiben, die definiert, auf welche Rechner ein Benutzer Zugriff haben soll, und darauf vertrauen, dass sie überall durchgesetzt wird. Anstatt SSH-Zertifikate zu verwalten (die langlebig und schwer zu widerrufen sind), kann das Unternehmen Entwicklern erlauben, sich mit den gleichen Google-Anmeldeinformationen anzumelden, die sie überall sonst verwenden.

Wenn ein Entwickler das Unternehmen verlässt, kann es diese Anmeldedaten sofort widerrufen, wodurch es sich keine Sorgen über eventuell noch vorhandene öffentliche Schlüssel machen muss.

Mit Cloudflare Access können die Entwickler von Replicated problemlos mehrere Umgebungen einrichten (um z. B. eine neue k8s-Version auszuprobieren), und sie benötigen dafür nicht die größten und leistungsfähigsten Laptops. Sie können auch ihr lokales Betriebssystem und ihre lokale Umgebung (MacOS, Windows, Linux) wählen, da jede Version unterstützt wird, solange SSH ebenfalls unterstützt wird. Und da der Code nicht auf dem Laptop des Entwicklers gespeichert ist, begibt er sich auch nicht mit ihm in Cafés oder an andere unsichere Orte. Dies ist ein entscheidender Sicherheitsvorteil, da der Verlust eines Laptops nicht mehr bedeutet, dass dadurch möglicherweise die Codebasis kompromittiert wird.

„Mithilfe von Cloudflare Access und Argo Tunnel ist jede einzelne Entwicklungsumgebung zu einem Ort der Zusammenarbeit geworden", so Campbell und Miller. „Das ist großartig, wenn sich zwei Entwickler nicht im selben Raum befinden. Außerdem sind wir weniger an unsere Entwicklungsumgebungen gebunden – wenn mein Server aus unbekannten Gründen nicht richtig funktioniert, kann ich ihn einfach löschen und einen neuen, sauberen Server bekommen, anstatt stundenlang zu versuchen, das Problem zu beheben."